

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION**

CELLEBRITE MOBILE SYNCHRONIZATION LTD.,
and CELLEBRITE USA, INC.

Plaintiff.

v.

MICRO SYSTEMATION AB, and
MSAB, INC.

Defendants.

Civil Action No. ____-cv-____

**SECOND EXPERT
DECLARATION OF ROBERT
ZEIDMAN**

ECF Case

CONFIDENTIAL

Table of Contents

I.	Summary of Findings.....	1
II.	Scope of report.....	1
III.	Cellebrite’s Copyright Infringement Claim	1
A.	Cellebrite Did Apply Accepted Methodology For Determining Substantial Similarity In The Context Of Software Code.....	1
B.	Application Of The Successive Filtration Approach Demonstrates That Cellebrite Can Establish Substantial Similarity	3
1.	Similarities Between Bootloaders Are Not Dictated By External Considerations.....	3
2.	Similarities In Configuration File (“Cellebrite,” “dunno about the rest,” etc.) Are Not Trivial.....	4
3.	The Presence Of “NAND,” “PRBN,” And “INTN” Inside QCDumper.dll Is Not Trivial.....	5
4.	The “Communication Signatures” Are Significant Signs of Copying	5
5.	The 0xB7 Samsung Command (“Magic Code”) Is Not Common In The Industry	6
6.	The Loading Addresses Are Significant Signs of Copying.....	6
7.	The Model Search Algorithm Is Not In The Public Domain	6
8.	MSAB’s Stack-Changer Are Not Dictated By Function.....	7
9.	Patching Of The AES Encryption Function Is A Significant Sign of Copying	7
10.	Selection Of Command 8 Was Not Dictated By Logic And Convenience	7
11.	Selection Of Address Offsets Was Not Dictated By Logic And Convenience	8
12.	The USB Communications And Cache Functions Were Not Dictated By Logic And Convenience.....	9
13.	The OneNAND Initialization Is Unnecessary And Trivial	9
14.	The “Ownership String” Is Not Trivial	9
C.	Cellebrite’s Trade Secret Misappropriation Claim	10
1.	Cellebrite Can Establish That The Subject Information Is Its Trade Secret	10
D.	The Law Also Supports That Reverse Engineering Is Not Misappropriation	11
E.	Differences Do Not Negate copying	11
IV.	Conclusion	11

I, Robert Zeidman, provide the following expert disclosures.

I. SUMMARY OF FINDINGS

1. MSAB has submitted to the court a memorandum that enumerates their reasons why they claim they did not infringe Cellebrite's copyright or misappropriate Cellebrite's trade secrets. I find their reasoning to be faulty, and I stand by my original declaration without any changes.

II. SCOPE OF REPORT

2. Based on my background and experience, I have been asked by the law firm of Pearl Cohen Zedek Latzer Baratz LLP, on behalf of Cellebrite Mobile Synchronization Ltd. ("Cellebrite"), to respond to the *Declaration Of Örjan Gatu In Opposition To Application For A Temporary Restraining Order* and *Defendants' Memorandum In Opposition To Plaintiffs' Motion For Temporary Restraining Order*.

III. CELLEBRITE'S COPYRIGHT INFRINGEMENT CLAIM

3. MSAB states that Cellebrite does not have a valid copyright claim for the reasons below. I will address each reason individually.

A. CELLEBRITE DID APPLY ACCEPTED METHODOLOGY FOR DETERMINING SUBSTANTIAL SIMILARITY IN THE CONTEXT OF SOFTWARE CODE

4. MSAB claims that Cellebrite did not apply accepted methodology for determining substantial similarity in the context of software code, but this is not correct. In their arguments, they rely on the book *Nimmer on Copyright*, but in doing so they rely on generalities about software code that do not apply in this case.
5. For example, Nimmer states that "Authors of computer programs do not always have the broad range of choices of expression." This is true, but in my declaration I showed that

MSAB had numerous choices and gave examples of them. It is therefore evidence of copying that many choices were identical to those of Cellebrite, a fact that MSAB admits in their responses but attribute to coincidence or claim that no other choices would be reasonable. It is my opinion that many of the other choices would have been reasonable as I stated in my declaration and as I explain in the sections below.

6. Nimmer states, “External factors, such as the computer on which the program is to run, the other software with which the program must interact, and the nature of the problem to be solved dictate many aspects of a program’s design, structure, or actual code.” Again, this is true, but the aspects of the Cellebrite program and the MSAB program that are similar or identical are in places where external factors played no part as I stated in my declaration and as I explain in the sections below. Those parts of the code that were in fact dictated by external factors were not included in my declaration.
7. Nimmer states, “An extensive body of computer science literature, rather than the individual programmer’s creativity, provides numerous common programming techniques found in a wide variety of programs.” Again, this is true, but the aspects of the Cellebrite program and the MSAB program that are similar or identical are in places that did not involve common algorithms or well-known techniques as I stated in my declaration and as I explain in the sections below. Those parts of the code that did involve common algorithms or well-known techniques were not included in my declaration.
8. Nimmer states, “[B]y successively filtering out unprotected material, a core of protected material remains, against which the court can compare the allegedly infringing program.” This is also true and it is part of my consulting firm’s written process to perform this filtering. The results in my declaration are only those similarities that remained after such filtering was performed.

**B. APPLICATION OF THE SUCCESSIVE FILTRATION APPROACH
DEMONSTRATES THAT CELLEBRITE CAN ESTABLISH SUBSTANTIAL
SIMILARITY**

9. MSAB states that “among the software material that must be filtered out as unprotected are program elements that are: (i) dictated by logic and efficiency; (ii) taken from the public; domain; and (iii) dictated by external considerations.” This is correct. They also reference the Abstraction Filtration Comparison (AFC) test established in the case of *Computer Assocs.Int’l, Inc. v. Altai, Inc.*, 982 F.2d 693, 709 (2d Cir. 1992). That test, however, applies to computer source code, but we do not have the source code from MSAB in order to do that comparison. Yet even in their memorandum, MSAB, quoting Nimmer, acknowledges that “[t]his filtration test ‘may now be regarded as the dominant, albeit not universal, standard.’” So MSAB cannot require Cellebrite to perform a test that is not a universal standard on source code that is not available. However, I performed filtration as it applies to executable binary code in general and to the programs in question here specifically and confirmed that copying occurred.

**1. SIMILARITIES BETWEEN BOOTLOADERS ARE NOT DICTATED BY
EXTERNAL CONSIDERATIONS**

10. MSAB claims that “much of bootloader operation and design is dictated by features and errors made by the manufacturer of the mobile phone. After all, both products are attacking the same firmware that contains the same properties and vulnerabilities.” This statement is a huge generalization that ignores the very specific implementation details that are not dictated by any considerations and for which there were many alternative solutions.
11. MSAB points out several times that the code of the bootloaders is of “miniscule size.” However, whether something is substantial is not based on its size but other factors such as how creative it is, how long it took to develop, how important it is to the marketplace, etc.

For example, if you found a stranger on your premises with a key to your house, you would not shrug it off because a key is a small piece of metal. You would not consider the situation based on how many keys the person had on them or determine that a key and a bottle cap were roughly the same weight and thus had the same miniscule importance. Rather you would look at the significance of the key to determine whether to be concerned, whether to suspect a crime had been committed, and whether to call the police.

12. MSAB states a number of times that their bootloaders have important differences compared to Cellebrite's. The issue is not how many differences there are, but how many similarities there are that cannot be explained by reasons other than copying. There are many.
13. Thus the similarities of the bootloaders comprise a significant sign that the bootloader code was copied.

2. SIMILARITIES IN CONFIGURATION FILE (“CELLEBRITE,” “DUNNO ABOUT THE REST,” ETC.) ARE NOT TRIVIAL

14. MSAB states that because a configuration file is not executable code, but simply a text file that resides on the PC side of MSAB'S product, that is it insignificant or not protectable. This is not true. A configuration file can be creative and thus protectable. A configuration file is important for configuring the software so that it runs correctly for the user. An incorrect configuration file can mean that the program will no execute at all and is thus very significant.
15. MSAB states that the part of the configuration file that appears copied from Cellebrite “pertains to a temporary testing configuration that was used internally at MSAB for performance comparison against the UFED.” However, MSAB offers no proof of this other than a statement by one of its engineers and a diagram that does not reference the configuration file. Initial testing of MSAB's configuration file by Cellebrite appears to show that the configuration file is used during normal operation of MSAB's software, but I have not yet had time to confirm this.

16. Thus the similarities in the configuration files comprise a significant sign of copying.

**3. THE PRESENCE OF “NAND,” “PRBN,” AND “INTN” INSIDE
QCDUMPER.DLL IS NOT TRIVIAL**

17. MSAB claims that these strings representing Cellebrite commands were only used together with the configuration file in order to do the performance comparison described above, and were never operational code in any product released to any customer. However, there is no logical reason I can think of why unique commands used by Cellebrite in Cellebrite’s software would show up in MSAB’s software other than copying.

18. Also, MSAB offers no proof that these commands were used solely for performance testing other than a statement by one of its engineers, a diagram that does not reference the commands, and some isolated code snippets that cannot be judged out of context. I do not find MSAB’s reason plausible.

19. Thus the use of “NAND,” “PRBN,” And “INTN” inside MSAB code is a significant sign that the code was copied.

**4. THE “COMMUNICATION SIGNATURES” ARE SIGNIFICANT SIGNS OF
COPYING**

20. The “communication signatures” in question are ways of identifying particular functions in Samsung’s code, but MSAB obscures the issue by referring to Samsung’s code and not to the signatures themselves. There are many ways of identifying code just as there are many ways of identifying people. For example, people may be identified by their name, their address, their fingerprint, their social security number, or their signature. For code, it is common to use a mathematical representation such as a checksum or a CRC. It is not common to use the specific method that Cellebrite uses and therefore it is a sign of copying that MSAB chose the same unusual means of identification.

5. THE 0XB7 SAMSUNG COMMAND (“MAGIC CODE”) IS NOT COMMON IN THE INDUSTRY

21. MSAB again obfuscates the issue by addressing the command itself, a simple number, rather than the fact that both MSAB and Cellebrite use this same number. MSAB simply states that “the 0xB7 command, referred to as the ‘Magic Code’ by Cellebrite, is a command that is defined as unused by the Samsung code.” However, MSAB never explains how it came to use the same code that Cellebrite uses when there are many other choices available. The command itself may not be significant, but the fact that both programs use this same command when other choices were available is a significant sign of copying.

6. THE LOADING ADDRESSES ARE SIGNIFICANT SIGNS OF COPYING

22. MSAB claims “this is not executable code, but rather a property of the mobile phone as created by Samsung.” Again MSAB obfuscates the issue by focusing on the address itself rather than the fact that both MSAB and Cellebrite use this same address. MSAB gives no logical reasons for choosing these addresses and does not explain how out of the many arbitrary possibilities for these addresses, their programmer chose the exact same ones as the Cellebrite programmer.
23. The fact that both programs use the same loading addresses when other choices were available is a significant sign of copying.

7. THE MODEL SEARCH ALGORITHM IS NOT IN THE PUBLIC DOMAIN

24. MSAB significantly oversimplifies, and thus minimizes the issue of the search algorithm by stating “the algorithm is a simple one-pass loop that compares data. It is a very common operation in software development to make simple loops to compare data, and software programs routinely implement comparisons within loops.” Yes, many algorithms use loops and probably every program ever written has a loop. But the specifics of creating signatures

for specific functions and then looking for those signatures to determine the phone model are used by both programs.

25. The fact that both programs use the same model search algorithm when other algorithms were available is a significant sign of copying.

8. MSAB'S STACK-CHANGER ARE NOT DICTATED BY FUNCTION

26. MSAB claims that the stack change function "is a small function that exploits a specific vulnerability in RIM's BlackBerry code." First, the size of the function is not significant. The importance of the function is significant and as I explained in my declaration, this function is important. While it is true that the stack changer function takes advantage of a vulnerability in RIM's BlackBerry, discovering this vulnerability took significant time and then figuring out how to write code to exploit this vulnerability for the specific use of loading a custom bootloader also took significant time.
27. The fact that both programs use the same essential stack changer function that was very difficult to develop is a significant sign of copying.

9. PATCHING OF THE AES ENCRYPTION FUNCTION IS A SIGNIFICANT SIGN OF COPYING

28. MSAB claims that "the AES encryption is part of the BlackBerry operating system, and just represents a suitable and reasonable point for MSAB to inject code." That may be true, but as I point out in my declaration, there were other functions that could have been patched. The fact that MSAB chose the same function as Cellebrite is a significant sign of copying.

10. SELECTION OF COMMAND 8 WAS NOT DICTATED BY LOGIC AND CONVENIENCE

29. MSAB claims states:

Command 8 is not arbitrarily chosen at all, but is in fact the first suitable command encountered if starting from Command 1 and testing each command upwards, which is a reasonable process to use. This means that the address for Command 8 can be modified with a bootloader and still be able to exit without causing any problems for the main loader. As such, MSAB's choice of Command 8 was not random. Instead it was the first command MSAB's developer could choose.

30. However, a programmer could choose the first command available or, for example the last command available. Or the programmer could have chosen any of the other available commands. Especially in light of all of the other signs of copying, the fact that MSAB chose the same unused command as Cellebrite is a significant sign of copying.

11. SELECTION OF ADDRESS OFFSETS WAS NOT DICTATED BY LOGIC AND CONVENIENCE

31. MSAB states:

An address offset is not executable code, but rather a property of the mobile phone. It is dependent on the firmware created by Blackberry. The first address (0x18000000) was a given to start with, but the two other addresses (0x18018000 and 0x18024000) were not chosen at random either. Instead they were the combined result of a logical thought process and the specifics of the BlackBerry platform.

32. Again, MSAB attempts to cloud the issue by focusing on the address offsets themselves and not the suspicious situation where both MSAB and Cellebrite chose the same exact addresses. In the explanation given by MSAB, they explain the similarities, when many options were available, by talking about rounding numbers up and then choosing an arbitrary offset. However, MSAB never explains how the numbers were rounded up to the same exact numbers used by Cellebrite or how the arbitrary offset turned out to be the exact same as the arbitrary offset used by Cellebrite.
33. The fact that both programs use the same three addresses when other choices were available is a significant sign of copying.

**12. THE USB COMMUNICATIONS AND CACHE FUNCTIONS WERE NOT
DICTATED BY LOGIC AND CONVENIENCE**

34. MSAB again clouds the issue by claiming “these functions are provided as a part of the BlackBerry operating system and were written by Blackberry and not by Cellebrite. The bootloader uses these functions in order to send data back to the PC.” The significance is not the BlackBerry functions themselves, but the fact that both programs use the same specific parameters for these functions.
35. The fact that both programs use the same parameters is a significant sign of copying.

13. THE ONENAND INITIALIZATION IS UNNECESSARY AND TRIVIAL

36. MSAB attempts to explain the fact that the same unnecessary command is found in both Cellebrite and MSAB’s programs by stating:

MSAB’s developer misread the specifications for the memory chip, and believed an unnecessary command was a necessary command to unlock the NAND-block array of the memory chip on the Blackberry. It is clear that this is a mistake because MSAB’s developer repeated the mistake throughout other parts of the code. Gatu Decl. ¶ 54. It is purely a coincidence that this command is present in Cellebrite’s code, unless Cellebrite originally made the same mistake.

37. This is a strange explanation. It seems to be saying that the programmers at Cellebrite and MSAB both made the same exact mistake based on the same exact misunderstanding and that both programmers left this mistake in their programs. I do not believe this is a reasonable explanation.
38. The fact that both programs incorporate the same unnecessary command is a significant sign of copying.

14. THE “OWNERSHIP STRING” IS NOT TRIVIAL

39. While MSAB’s statement that “the ownership string does not constitute code and has absolutely zero influence on the function of the program” is true, that is not the point. The

fact that both programs contain very similar ownership strings is a significant sign of copying.

C. CELLEBRITE'S TRADE SECRET MISAPPROPRIATION CLAIM

40. MSAB state that Cellebrite does not have a valid trade secret misappropriation claim. I address their points that regard to technical issues in the sections below.

1. CELLEBRITE CAN ESTABLISH THAT THE SUBJECT INFORMATION IS ITS TRADE SECRET

41. MSAB claims that “a vulnerability is not a formula, pattern, compilation, program, device, method, technique, or process—rather it is a fact. The location of vulnerabilities of third party mobile devices is not Cellebrite’s to own, and therefore, is not a trade secret.” This may technically be true, but it is beside the point. The trade secret that Cellebrite is claiming is not the vulnerability itself, but the code used to exploit that vulnerability. As I pointed out in my declaration and in the sections above, there is significant evidence that the code that Cellebrite developed to exploit this vulnerability has been copied by MSAB.
42. MSAB claims that “the model signature search algorithm is a simple one-pass loop that compares data” and is thus not a trade secret. As I stated before, this greatly oversimplifies the model search algorithm used by Cellebrite and that I believe was copied by MSAB.
43. MSAB similarly claims “not only is Command 8 code that was written and implemented by BlackBerry, Command 8 is also the first command capable of executing an extraction payload if one were to test the commands sequentially beginning at “Command 1.” Again, the command itself may not be a trade secret of Cellebrite, but Cellebrite’s code to use this command can be a trade secret.
44. Overall, MSAB has oversimplified and minimized the functionality of the code that Cellebrite has developed in order to claim that it is not protectable as trade secrets. I disagree. The code is significant. MSAB has also misinterpreted Cellebrite’s trade secrets

as code within the respective smartphones rather than correctly stating that Cellebrite's trade secrets are code that exploits code within the smartphones.

D. THE LAW ALSO SUPPORTS THAT REVERSE ENGINEERING IS NOT MISAPPROPRIATION

45. MSAB state that "the law is also well-established that 'reverse engineering' of publicly available information does not constitute trade secret misappropriation or violate the UTSA." This is true. However, as stated in the decision in *Atari, Inc. v. Nintendo of America, Inc.*, 975 F.2d 832, 24 U.S.P.Q.2d (BNA) 1015 (Fed. Cir. 1992), a clean room development procedure must be used to ensure that no copyrights are infringed when creating new code from reverse-engineered code. MSAB has offered no statement claiming that a clean room procedure was used.
46. Also, this argument by MSAB is confusing because MSAB states clearly in their memorandum that they did not reverse engineer Cellebrite's code. They state "the allegation that MSAB reverse engineered Cellebrite's product is not accurate." Similarly Orjan Guta, in his declaration, states that there was no reverse engineering and no copying of code.

E. DIFFERENCES DO NOT NEGATE COPYING

47. MSAB points out a number of differences between MSAB's solution and Cellebrite's solution. However, this is irrelevant and only serves to confuse the issue. Copyright infringement and trade secret misappropriation rests on what is similar and what was copied, not what parts may be different.

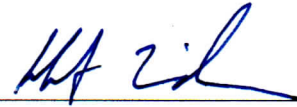
IV. CONCLUSION

48. MSAB has submitted to the court a memorandum that enumerates their reasons why they claim they did not infringe Cellebrite's copyright or misappropriate Cellebrite's trade

secrets. I find their reasoning to be faulty, and I stand by my original declaration without any changes.

49. It is my understanding that this case is at its initial stages and that discovery in this case will be undertaken shortly. Accordingly, I reserve the right to supplement or amend my opinions in light of any additional evidence, testimony, or information that may be provided to me after the date of this report. I also reserve the right to supplement or amend my opinions in response to any expert reports served by any other party in the lawsuit.

Dated: August 23, 2013



Robert Zeidman

Dated: August 23, 2013

Respectfully submitted

**CELLEBRITE MOBILE
SYNCHRONIZATION, LTD., ET AL.
By Counsel**

/s/

Bernard J. DiMuro, Esq.
VSB #18784
Counsel for Plaintiffs
DiMUROGINSBERG, PC
1101 King Street, Suite 610
Alexandria, Virginia 23314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
E-mail: bdimuro@dimuro.com

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and accurate copy of the foregoing was sent by e-mail and first, class, postage prepaid mail this 23rd day of August, 2013 to:

Damon Wright, Esquire
dwdwright@venable.com
Venable, LLP
575 7th Street, NW
Washington, DC 20004
T: 202.344.4000
F: 202.344.8300

David A. Wilson, Esquire
Thompson Hine, LLP
David.wilson@thompsonhine.com
1919 M Street, N.W., Suite 700
Washington, DC 20036-3537
T: 202.331.8800
F: 202.331.8330

Counsel for Defendants

/s/

Bernard J. DiMuro, Esq.

VSB #18784

Counsel for Plaintiffs

DiMUROGINSBERG, PC

1101 King Street, Suite 610

Alexandria, Virginia 22314

Telephone: (703) 684-4333

Facsimile: (703) 548-3181

E-mail: bdimuro@dimuro.com